Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): NAI1P503/00.147.01

I hereby certify that this correspondence is being e-filed with the USPTO on May 7, 2007

Signature /April Skovmand/

Typed or printed name April Skovmand

Application Number	Filed
09/785,216	02/20/2001

First Named Inventor: Lee Codel Lawson Tarbotton

Art Unit	Examiner
2131	Chai, Longbit

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- ☐ applicant/inventor.
- ☐ assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- ☑ attorney or agent of record. Registration number 41,429
- ☐ attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

/KEVINZILKA/
Signature

Kevin J. Zilka
Typed or printed name

408-971-2573
Telephone number

May 7, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☑ *Total of 1 forms are submitted.

REMARKS

The Examiner has rejected Claims 1, 4, 7-8, 11, 14-15, 18 and 21 under 35 U.S.C. 102(b) as being anticipated by Arnold (U.S. Patent No. 5,440,723). Additionally, the Examiner has rejected Claims 5-6, 12-13, and 19-20 under 35 U.S.C. 103(a) as being unpatentable over Arnold, in view of Waldin (U.S. Patent No. 6,094,731). Applicant respectfully disagrees with such rejections.

With respect to the independent claims, the Examiner has relied on Col. 23, lines 23-33, and lines 40-45; Col. 24, lines 21-26, and lines 45-57; and Col. 29, lines 36-38 from the Arnold reference to make a prior art showing of applicant's claimed technique "wherein said warning generating logic can generate a plurality of different types of warnings to said user that said target computer file may have suffered irreparable damage and said library includes data specifying which of said plurality of types of warnings should be issued in response to a particular detected computer virus" (see this or similar, but not necessarily identical language in the independent claims). Applicant's arguments made on page 7, third paragraph, through page 9, first paragraph of Amendment C mailed 11/13/2006 are hereby incorporated by reference.

In the Office Action dated 02/07/2007, the Examiner has argued that Col. 29, lines 26-32 of Arnold teach that "warnings may include the existence and the signature of the entity," including "whether or not the undesired software entity has been removed and… the particular signature of the virus [that] has been identified." Further, the Examiner has argued that Col. 24, lines 45-57 of Arnold teach that "warnings may describe… whether a virus can be removed or not as well as… whether the infected file can be restored / recovered or not." Additionally, the Examiner has noted that "a library is merely a collection of computer data structures and utilities that can be used by computer application programs as needed."

Applicant respectfully disagrees and points out that the excerpts relied on by the Examiner merely teach "killing or removing the undesirable software entity, and also possibly informing neighboring data processors of the existence and signature of the entity" (Col. 29, lines 29-32 – emphasis added). Further, the excerpts relied on by the Examiner teach a virus is removed if "the virus is an exact copy of one that [the system] is capable of removing" (Col. 24, lines 48-49). Further still, the excerpts teach that "[i]f the virus cannot be removed [in the above manner]… an automatic restore from a tape backup or from a read-only directory on a server, or

from another machine on the network is attempted" and that "[i]f an automatic restoration of the infected file cannot be accomplished, the user receives a message describing the situation, with instructions for manually restoring the file from backup" (Col. 24, lines 50-57 – emphasis added).

However, merely disclosing the removal of an entity, and the informing of the existence and signature of the entity, as in Arnold, does not teach "a plurality of different types of warnings to said user that said target computer file may have suffered irreparable damage" (emphasis added), as claimed by applicant. Further, merely sending a message to a user disclosing instructions for manually restoring the file when a virus is not an exact copy of a virus the system is capable of removing, and when the file was unable to be automatically restored, as in Arnold, fails to disclose "warning generating logic [which] can generate a plurality of different types of warnings to said user that said target computer file may have suffered irreparable damage" (emphasis added), as claimed by applicant. Moreover, none of the excerpts relied upon by the Examiner even suggest a "library [which] includes data specifying which of said plurality of types of warnings should be issued in response to a particular detected computer virus" (emphasis added), as claimed by applicant.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 4 et al., the Examiner has relied on Col. 23, lines 41-42; Col. 24, lines 12-15, and lines 45-57; and Fig. 3, elements F, J, K, O, and G from the Arnold reference to make a prior art showing of applicant's claimed technique "wherein said warning to said user that said target computer file may have suffered irreparable damage includes an option to add a notification message into said target computer file." Applicant's arguments made on page 10, first through third paragraphs, of Amendment C mailed 11/13/2006 are hereby incorporated by reference.

In the Office Action dated 02/07/2007, the Examiner has argued that Col. 24, lines 45-57 of Arnold teach that "additionally, a warning message can be added, describing the situations including… whether a virus can be removed or not as well as… whether the infected file can be restored / recovered or not." The Examiner has further asserted that "the situation would evidently include the target computer file affected by the virus."

Applicant respectfully disagrees and notes that the excerpts relied on by the Examiner merely teach that a virus is removed if "the virus is an exact copy of one that [the system] is

capable of removing" (Col. 24, lines 48-49). Additionally, the excerpts teach that "[i]f the virus cannot be removed [in the above manner]… an automatic restore from a tape backup or from a read-only directory on a server, or from another machine on the network is attempted" and that "[i]f an automatic restoration of the infected file cannot be accomplished, the user receives a message describing the situation, with instructions for manually restoring the file from backup" (Col. 24, lines 50-57 – emphasis added).

However, merely sending a message to a user disclosing instructions for manually restoring the file when a virus is not an exact copy of a virus the system is capable of removing, and when the file was unable to be automatically restored, as in Arnold, fails to even suggest a technique "wherein said warning to said user that said target computer file may have suffered irreparable damage includes an option to **add** a notification message **into** said target computer file" (emphasis added), as claimed by applicant. Clearly, sending a message to a user, as in Arnold, fails to suggest "an option to **add** a notification message **into** said target computer file" (emphasis added), in the manner as claimed by applicant.

With respect to Claim 5 et al., the Examiner has relied on Col. 6, lines 65-67 from the Waldin reference, in addition to Col. 24, lines 45-57; and Col. 29, lines 26-32 from the Arnold reference to make a prior art showing of applicant's claimed technique "wherein said notification message includes authentication data identifying said target computer file into which it was inserted." Applicant's arguments made on page 11, second through third paragraphs, of Amendment C mailed 11/13/2006 are hereby incorporated by reference.

In the Office Action dated 02/07/2007, the Examiner has argued that the Abstract and Col. 6, lines 57-67 of the "Waldin reference [are] relied upon [to provide] a digital signature validation to authenticate either a message or a file in an antivirus-enhanced computer system."

Applicant respectfully disagrees and points out that the excerpts relied on by the Examiner merely teach that "[a]n authentication module… affixes a digital signature to critical sectors file" and that the "[r]ecipient computer… decrypts the digital signature… produced by originating computer… to verify the authenticity of the contents of [the] critical sectors file" (Abstract – emphasis added). Further, the excerpts teach that an "authentication module… examines the authenticity of [a] digital signature" in order to determine if "the transmitted data

have been changed in some way and the entire contents of [the] file… must be rescanned for viruses" (Col. 6, lines 51-65 – emphasis added).

However, merely affixing a digital signature to a critical sectors file, and the examination of the authenticity of a digital signature file, as in Waldin, fails to even suggest a technique "wherein said notification message includes authentication data identifying said target computer file into which it was inserted" (emphasis added), as claimed by applicant.

Furthermore, Waldin discloses that "[i]f a virus is detected by module 3 (step 42), module 3 typically informs the user, by sending a message via user interface 7, e.g., a monitor (step 43)" and that "[i]f, on the other hand, module 3 does not detect a virus in file 1 (step 42), authentication module 12 is invoked to perform steps 44, 45, and 28" (Col. 5, lines 1-6 – emphasis added). Moreover, Waldin discloses that '[i]n step 28, authentication module 12 produces the digital signature 15 of the file 4," and '[i]n sub-step 49, the digital signature 15 is "attached" to the original file 1…as described above in conjunction with step 45' (Col. 5, lines 28-50 – emphasis added).

However, disclosing that the authentication module attaches the digital signature to the original file when the module does **not** detect a virus, as in Waldin, clearly *teaches away* from applicant's claimed technique "wherein said warning to said user that said target computer file may have **suffered irreparable damage** includes an option to **add** a notification message **into** said target computer file" (see Claim 4 emphasis added), where "said notification message includes authentication data identifying said target computer file into which it was inserted" (Claim 5 – emphasis added), in the context as claimed by applicant. Clearly, Waldin's disclosure of attaching the digital signature of the file when a virus is not detected, simply *teaches away* from a "notification message includ[ing] authentication data identifying said target computer file into which it was inserted" where "said target computer file may have suffered irreparable damage" (emphasis added), in the context as claimed by applicant.

With respect to Claim 6 et al., the Examiner has relied on Col. 6, lines 50-67 from the Waldin reference to make a prior art showing of applicant's claimed technique "wherein said notification message includes an electronic signature applied by said warning generating logic."

Applicant respectfully asserts that the excerpt relied upon by the Examiner merely teaches that "authentication module 12' examines the authenticity of digital signature 15." Further, the excerpt teaches that the authentication module "decodes the encoded digital signature," "decrypts the digital signature… producing a decrypted message digest," "calculates a new message digest of the contents of critical sectors file 4," and compares "the decrypted message digest… with the calculated message digest" in order to determine if "the transmitted data have been changed in some way and the entire contents of file 1 must be rescanned for viruses." Further, the excerpt also teaches that "[i]f the decrypted transmitted message digest is identical to the calculated message digest, the contents of file 1 are deemed by authentication module 12' to be 'unchanged in a way that could allow for a viral infection'" (Col. 6, line 65 – Col. 7, line 2).

Applicant respectfully asserts that decoding an encoded signature, decrypting the signature to produce a decrypted message digest, calculating a new message digest, and comparing the decrypted message digest to the calculated message digest in order to determine if a virus rescan is necessary, as in Waldin, in no way teaches a notification message, much less a technique "wherein said notification message includes an electronic signature applied by said warning generating logic" (emphasis added), as claimed by applicant.

In the Office Action mailed 02/07/2007, the Examiner failed to respond to applicant's arguments with respect to applicant's claimed technique "wherein said notification message includes an electronic signature applied by said warning generating logic." Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.